Security Operation Center (SOC) – starosti bezpečnostného manažéra

LYNX – spoločnosť s ručením obmedzeným Košice

Ján Odzgan

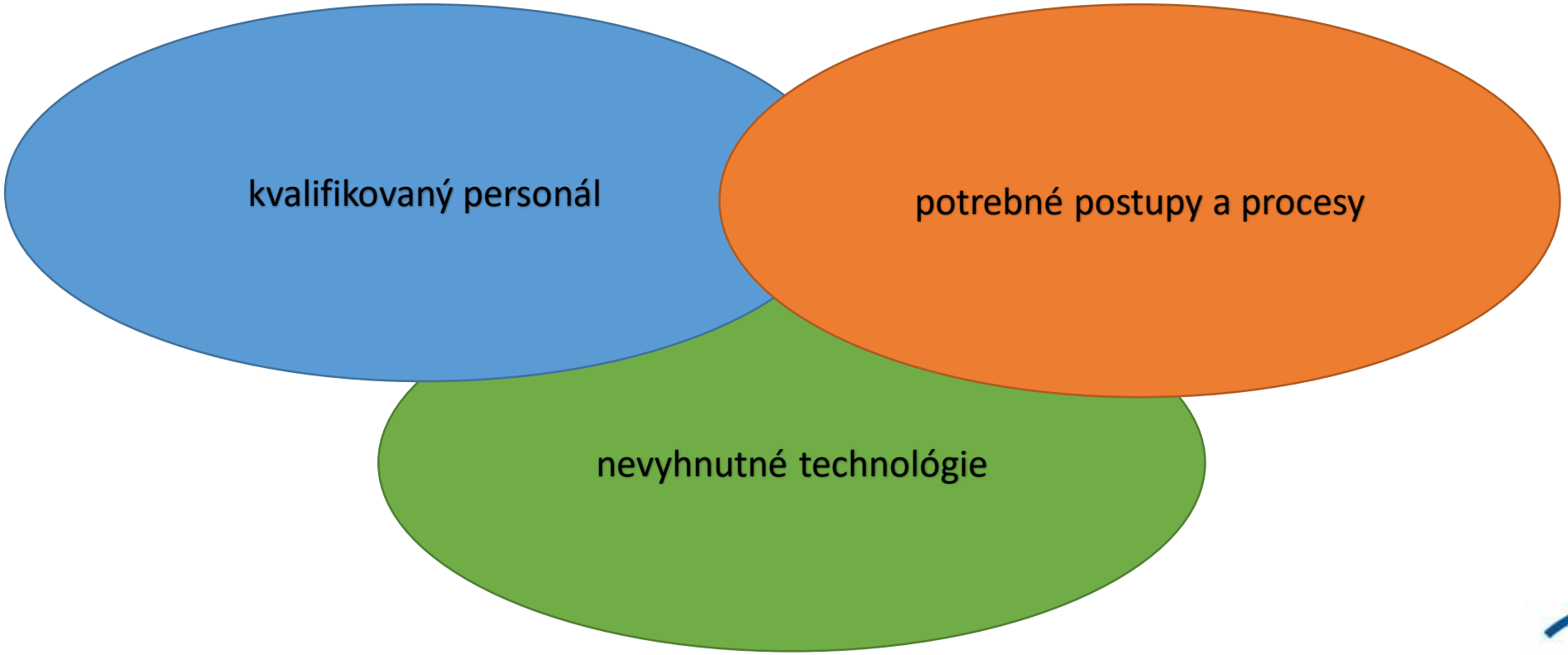
bezpečnostný špecialista (SIEM, NGFW, WAF, IPS, pentest)

LYNX – spoločnosť s ručením obmedzeným Košice

Obsah

- Security operation center - SOC
- SOC - architektúra služieb
- SOC - prehľad (survey) 2019 (SANS)
- SOC - problémy spojené s budovaním a prevádzkou
- SOC - odporúčania

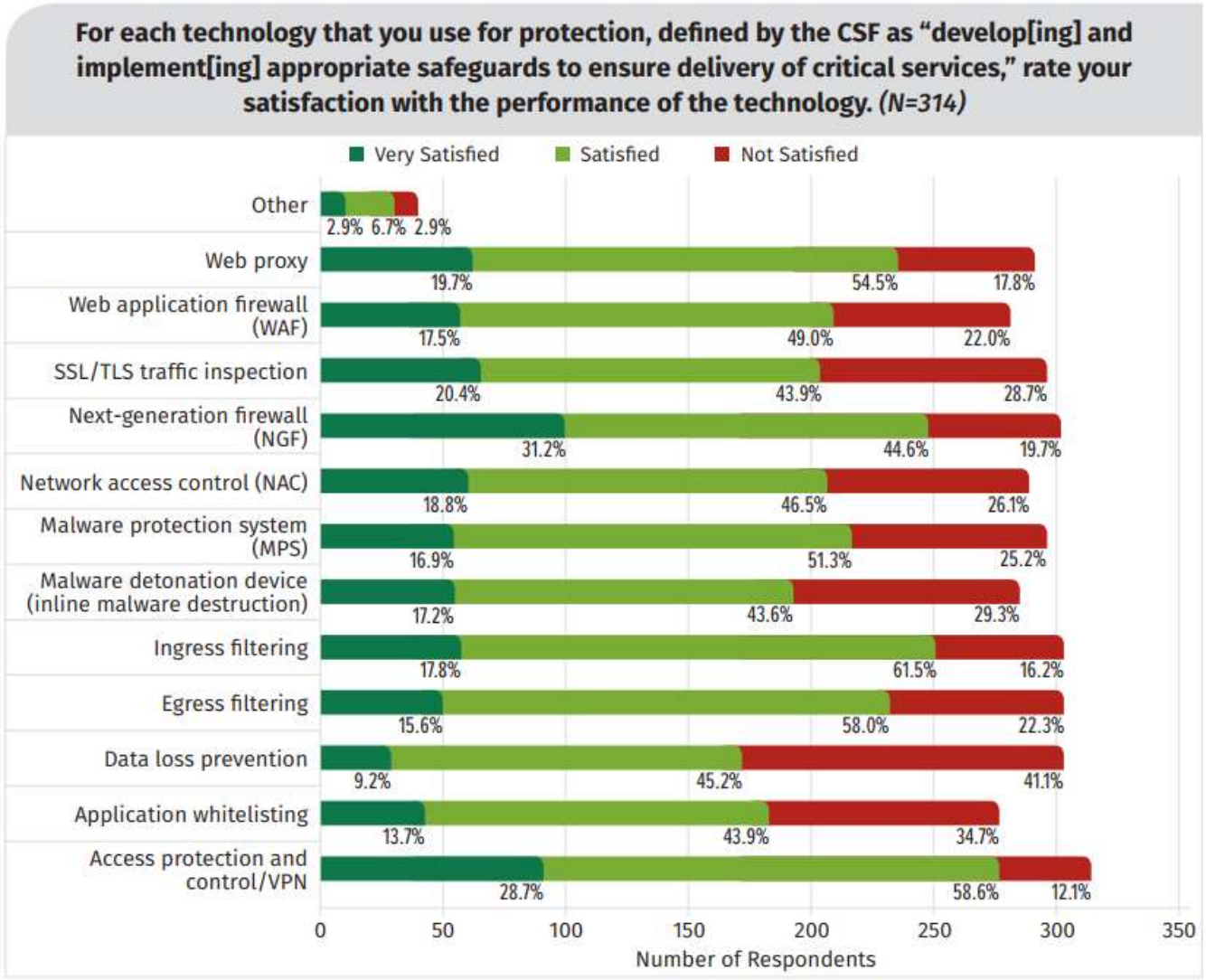
Security operation center - SOC



SOC - Architektúra služieb

SOC - survey 2019 (SANS)

Protection



https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - survey 2019 (SANS)

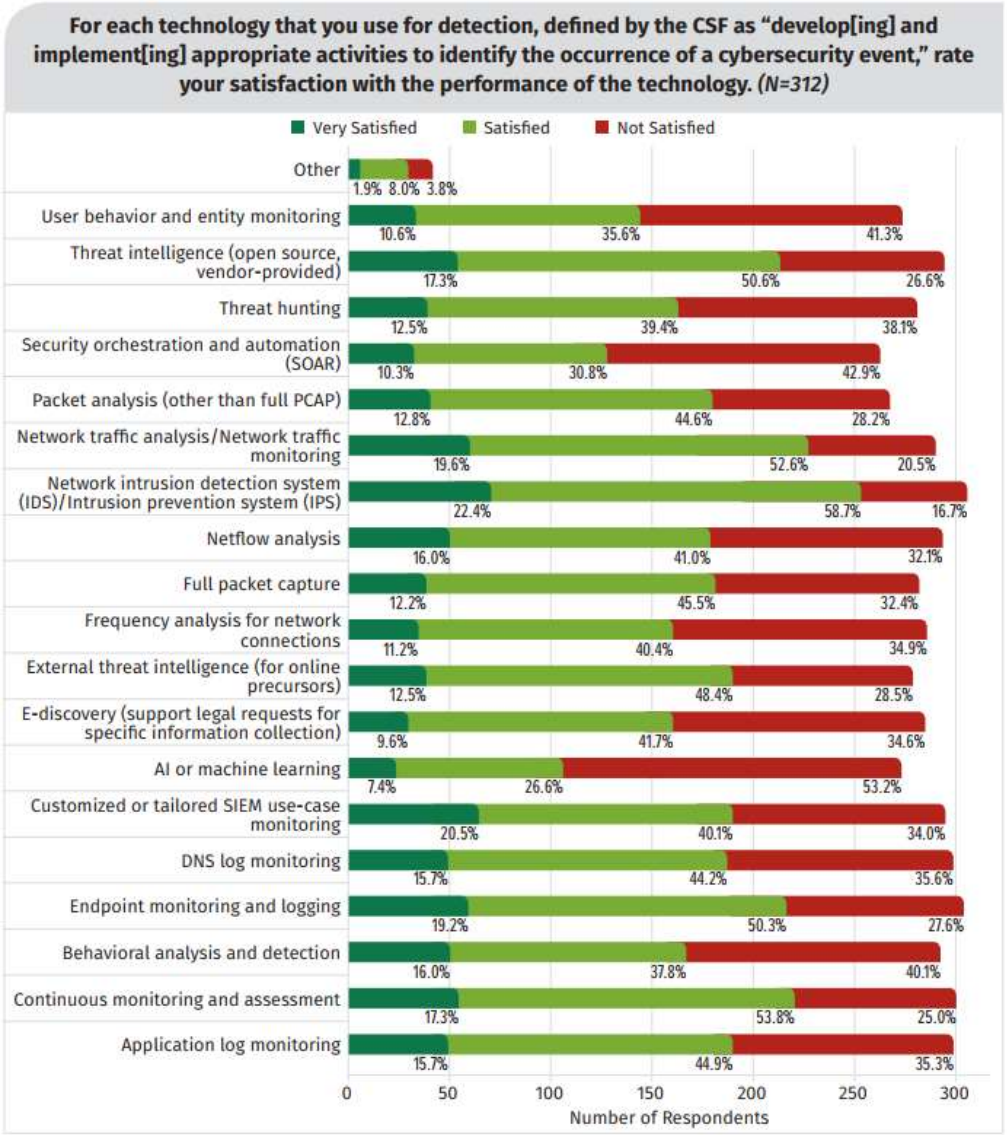
Protection

- Access control systémy a VPN vyhodnotená najlepšie
- NGFW a web proxy tiež veľmi vhodné
- DLP vyhodnotená najhoršie (nasadenie a vyspelosť)

https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - survey 2019 (SANS)

Detection



https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - survey 2019 (SANS)

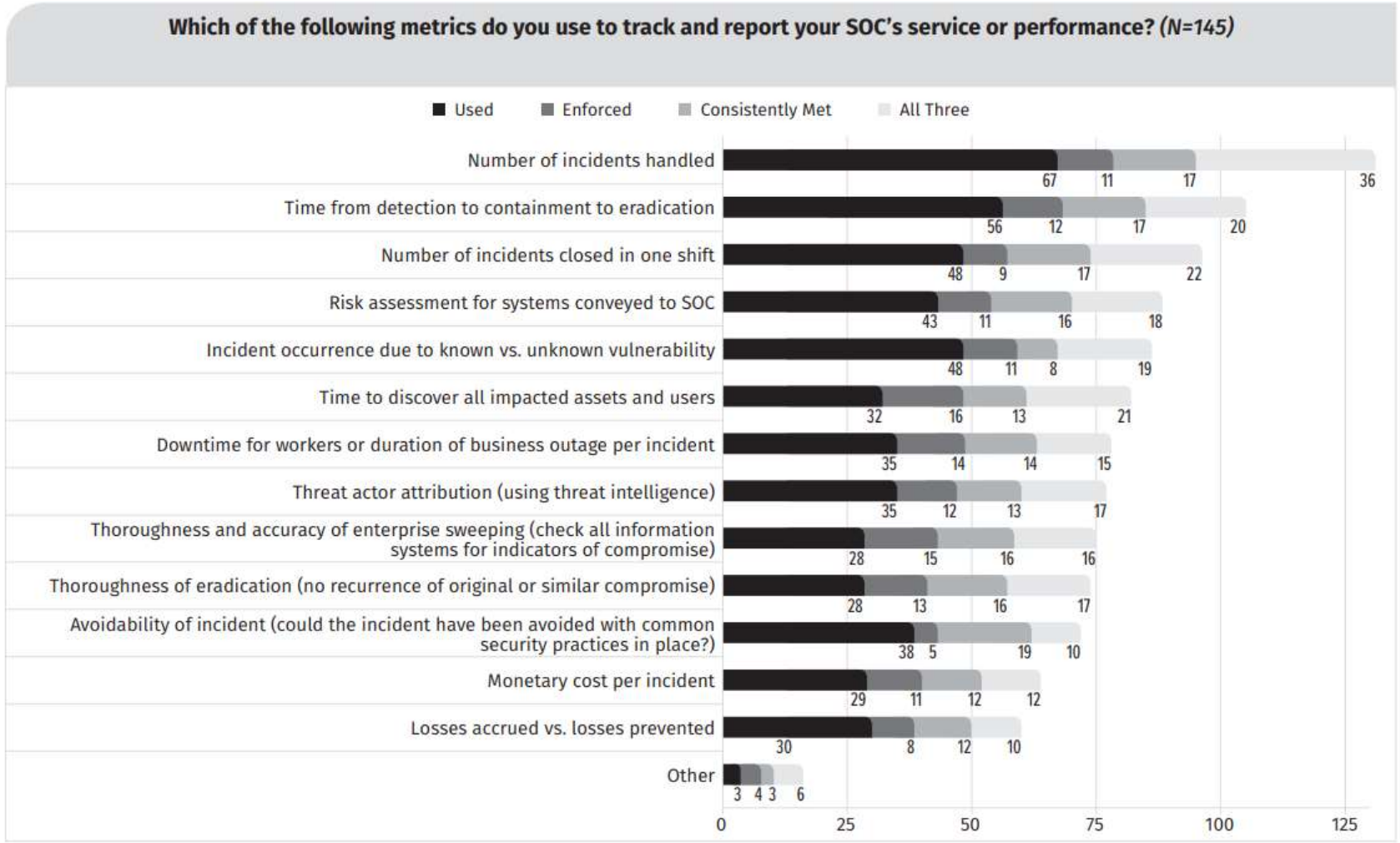
Detection

- IPS vyhodnotená najlepšie
- Network traffic monitoring, EDR, Threat intelligence a neustály monitoring tiež veľmi vhodné
- AI/machine learning vyhodnotená najhoršie (nasadenie a vyspelosť)

https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - survey 2019 (SANS)

Metrics



https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - survey 2019 (SANS)

Metrics

- počet všetkých incidentov
- čas od zistenia po odstránenie
- počet uzatvorených incidentov na jednej smene
- risk assessment pre systémy pripojených do SOC

https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - survey 2019 (SANS)

Problems

Table 4. Challenges to Full Integration and Utilization of a Centralized SOC Service Model Year-over-Year

	2019		2018	
Lack of skilled staff	57.7%	157	61.9%	148
Lack of automation and orchestration	49.6%	135	52.7%	126
Too many tools that are not integrated	43.0%	117	47.7%	114
Lack of management support	37.1%	101	37.2%	89
Lack of processes or playbooks	36.8%	100	42.7%	102
Lack of enterprisewide visibility	36.0%	98	41.8%	100
Too many alerts that we can't look into (lack of correlation between alerts)	32.0%	87	33.9%	81
Silo mentality between security, IR and operations	30.2%	82	30.1%	72
Lack of context related to what we are seeing	25.4%	69	18.8%	45
High staffing requirements	25.0%	68	27.2%	65
Regulatory or legal requirements	9.2%	25	12.6%	30
Other	4.8%	13	8.8%	21
Answered		**272**		**239**

https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

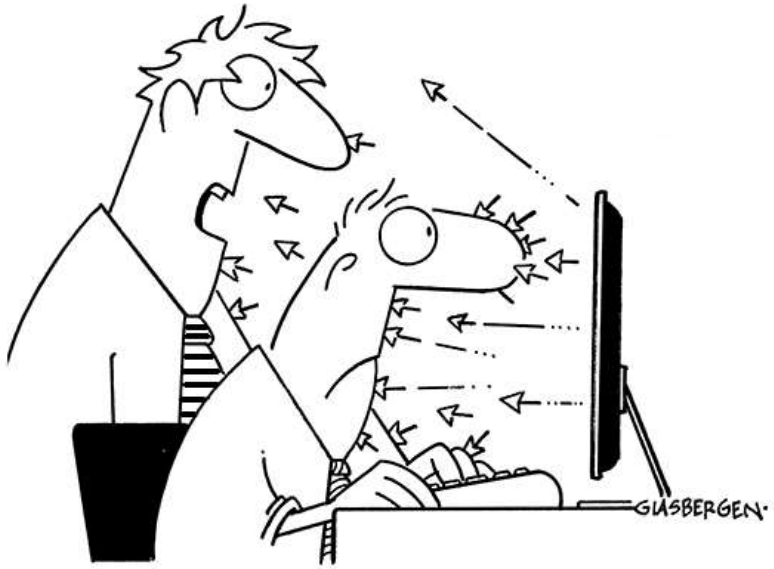
SOC - survey 2019 (SANS)

Problems

- nedostatok kvalifikovaného personálu
- nedostatočná automatizácia a orchestrácia spoločne s integráciou nástrojov
- nedostatočná podpora manažmentu organizácie
- nedostatky v procesoch a postupoch
- nedostatky vo viditeľnosti stavu bezpečnosti v celej organizácii a veľký počet incidentov

https://www.sans.org/reading-room/whitepapers/analyst/membership/39060

SOC - problémy spojené s budovaním a prevádzkou



"I'm no expert, but I think it's some kind of cyber attack!"

SOC - problémy spojené s budovaním a prevádzkou

Ľudia

- znalosti, skúsenosti a chýbajúci proces vzdelávania
- nedostatok časového priestoru, resp. nedostatok personálu

Technológie

- veľký počet rôznorodých systémov
- malá pridaná hodnota systémov a nedostatky v prepojení
- nedostatočná konfigurácia (bezpečnostných aj bežných systémov)

Procesy

- chýbajúce alebo zle definované postupy
- chýbajúce nástroje a procesy pre kooperáciu a riešenie aktivít SOC tímu
- nesprávne kritéria na hodnotenie SOC

"I'm no expert, but I think it's some kind of cyber attack!"

SOC - odporúčania

Procesy

- stanoviť správne biznis ciele pre SOC
- zabezpečiť správnu formu hodnotenia a prezentácie pridanej hodnoty
- identifikovať chránené aktíva, rozsah služieb a čas poskytovania služieb
- pred-pripraviť procesy a postupy (SOC manažér) a pravidelne ich aktualizovať

Ľudia

- zabezpečiť kvalifikovanú silu na riadenie (SOC manažér)
- správne rozhodnúť o forme SOC (outsourcing, hybrid alebo in-house)
- zaviesť mechanizmus na overenie vzdelávacieho procesu
- definovať správne role v tíme a zabezpečiť časovú dostupnosť (pozor na zdieľanie rolí)

Technológie

- identifikovať nedostatky v konfigurácii a architektúre existujúceho prostredia
- doplniť technológie s najväčším prínosom
- zabezpečiť technológie pre fungovanie SOC tímu (SIEM, threat intell, SOAR, KB a pod.)

SOC - LYNX – spoločnosť s ručením obmedzeným

MINISTERSTVO ZDRAVOTNÍCTVA SLOVENSKEJ REPUBLIKY

MINISTERSTVO OBRANY SLOVENSKEJ REPUBLIKY

NBÚ

MINISTERSTVO ŽIVOTNÉHO PROSTREDIA SLOVENSKEJ REPUBLIKY

MINISTERSTVO ZAHRANIČNÝCH VECÍ A EURÓPSKYCH ZÁLEŽITOSTÍ SLOVENSKEJ REPUBLIKY

VŠEOBECNÁ ZDRAVOTNÁ POISŤOVŇA

Finančná správa
Slovenská republika

Lynx – spoločnosť s ručením obmedzeným Košice
Gavlovičova 9
040 17 Košice

Ing. Ján Odzgan
tel: +421 905 767 951
e-mail: jan.odzgan@lynx.sk

Ďakujem za pozornosť